Terakreditasi SINTA Peringkat 4
Surat Keputusan Dirjen Penguatan Riset dan Pengembangan Ristek Dikti No. 28/E/KPT/2019
masa berlaku mulai Vol.3 No. 1 tahun 2018 s.d Vol. 7 No. 1 tahun 2022

Terbit online pada laman web jurnal:
http://publishing-widyagama.ac.id/ejournal-v2/index.php/jointecs

JOINTECS
(Journal of Information Technology and Computer Science)
Vol. 6 No. 3 (2021) 137 - 144
e-ISSN:2541-6448 p-ISSN:2541-3619

Forensik *Mobile* Pada Kasus *Cyber Fraud* Layanan *Signal Messenger* Menggunakan Metode NIST

Imam Riadi[1], Herman[2], Nur Hamida Siregar[3]
[1]Program Studi Sistem Informasi, Fakultas Sains dan Teknologi Terapan, Universitas Ahmad Dahlan
[2,3]Program Studi Informatika, Fakultas Teknologi Industri, Universitas Ahmad Dahlan
[1]imam.riadi@is.uad.ac.id, [2]hermankaha@mti.uad.ac.id, [3]nur2007048007@webmail.uad.ac.id

Abstract

The developments in the use of social media are currently experiencing a very rapid increase. One of the factors that increase the use of social media is the Covid-19 pandemic. All work activities are required and diverted to be done online. The use of social media has both positive and negative impacts. One of the negative impacts is the occurrence of crime. The purpose of this study was to obtain digital evidence in the form of text conversation data (chat), images, GIF, pdf document, video, voice call and video call by investigation with National Institute of Standard and Technology (NIST) method. The device used as the object of research is an android smartphone. The mobile forensic software used in this study is MOBILedit Forensic Express. Based on the results of forensic analysis, the performance of the MOBILedit Forensic tool is quite good because it can lift digital evidence in the form of 2 images, 1 GIF, 1 pdf document, and 1 video. The digital evidence obtained from this research had an overall success rate of 57,14%. This research got the result according to the expected goals even though not able to read chat, voice call and video call history.

Keywords: forensic; cybercrime; cyber fraud; signal messenger; NIST.

Abstrak

Perkembangan dalam penggunaan media sosial mengalami peningkatan yang sangat pesat saat ini. Salah satu faktor meningkatnya penggunaan media sosial yaitu pandemi Covid-19. Segala aktivitas pekerjaan diharuskan dan dialihkan untuk dikerjakan secara online. Aplikasi *Signal Messenger* memiliki fitur serupa *WhatsApp* (WA) tetapi lebih aman dari segi keamanan data pribadi. Keamanan data pribadi menjadi salah satu faktor beralihnya pengguna WA ke *signal messenger.* Penggunaan media sosial memiliki dampak positif dan dampak negatif. Salah satu contoh dampak negatif yaitu terjadinya tindak kejahatan. Tindak kejahatan dapat terjadi selama aplikasi yang digunakan menyediakan fitur untuk mengirim pesan teks, gambar maupun video. Aplikasi *signal messenger* juga memungkinkan disalahgunakan oleh individu yang tidak bertanggung jawab. Hal ini mendorong dilakukannya investigasi terhadap kasus *cyber fraud* melalui analisis forensik menggunakan pendekatan atau metode *National Institute of Standarts and Technology* (NIST). Tujuan penelitian ini yaitu mendapatkan barang bukti digital berupa data teks percakapan (chat), gambar, GIF, dokumen pdf, video, *voice call* dan *video call*. Perangkat yang digunakan sebagai objek penelitian berupa *smartphone* android. Perangkat lunak forensik mobile yang digunakan pada penelitian ini yaitu *MOBILedit Forensic Express*. Berdasarkan hasil analisis forensik, kinerja *tools MOBILedit Forensic* cukup baik karena mampu mengangkat bukti digital berupa 2 gambar, 1 GIF, 1 dokumen pdf, dan 1 video. Bukti digital yang diperoleh dari penelitian ini memiliki tingkat keberhasilan secara keseluruhan sebesar 57,14%. Barang bukti dapat digunakan sebagai pendukung penyelidikan tindak kejahatan kasus *cyber fraud* di pengadilan. Penelitian ini mendapatkan hasil sesuai tujuan yang diharapkan walaupun belum mampu membaca *chat,* histori *voice call* dan *video call*.

Kata kunci: forensik; cybercrime; cyber fraud; signal messenger; NIST.

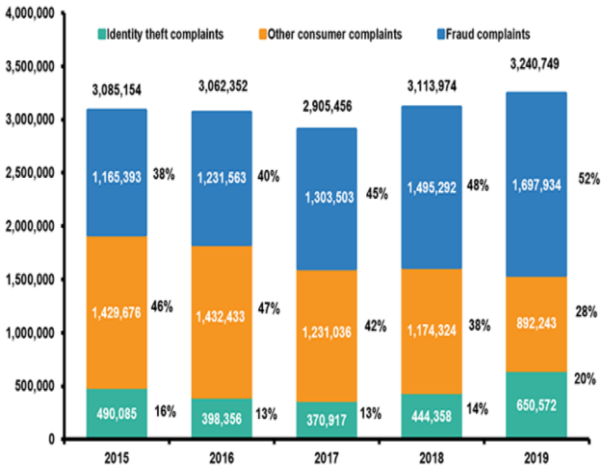
Diterima Redaksi : 19-07-2021 | Selesai Revisi : 21-08-2021 | Diterbitkan Online : 30-09-2021

1. Pendahuluan

Kehidupan saat ini telah memasuki era digital, sehingga aktivitas manusia sebagian besar dilaksanakan melalui berbagai media elektronik terutama yang berbasis internet termasuk media sosial. Berdasarkan data statistik pada Juli 2020, pengguna internet di dunia mencapai 3,96 milyar orang dengan peningkatan sebesar 10% dari tahun sebelumnya. Sementara pengguna internet di Indonesia mencapai 196,7 juta orang pada tahun 2020 hingga kuartal II. Hasil riset *We are social* Hootsuite menunjukkan pengguna media sosial aktif mencapai 150 juta atau 56% dari total populasi Indonesia di tahun 2020 [1].

Peningkatan penggunaan media sosial saat ini terjadi pada semua jenis media sosial selama pandemi. Pandemi Covid-19 mengharuskan segala aktivitas dilakukan secara *online*. Salah satu aplikasi media sosial yang menarik pengguna saat ini yaitu *Signal Messenger*. Aplikasi ini juga menyediakan layanan *Instant Messenger* (IM). *Signal Messenger* menjadi aplikasi gratis nomor 1 di Indonesia yang dapat ditemukan pada pencarian *Google Play Store* dan *Apple App* Store. Kepopuleran penggunaan dipengaruhi karena kekhawatiran dan kepedulian pengguna dalam menjaga informasi pribadi mereka.

Perkembangan yang pesat dalam penggunaan media sosial ini tidak hanya menimbulkan dampak positif tetapi juga dampak negatif, salah satunya tindak kejahatan (*cybercrime*). *Cybercrime* merupakan tindakan ilegal yang dilakukan menggunakan komputer atau perangkat elektronik lainnya [2]. Tindak kejahatan (*cybercrime*) dapat berupa penyebaran *hoax*, *cyberbullying*, penipuan, pemerasan, perdagangan manusia dan lainnya yang bisa berakibat fatal seperti tindakan pembunuhan. Survei statistik *Insurance Information Institute* dari tahun 2015 hingga 2019 menunjukkan beberapa kasus kejahatan dunia maya (*Cybercrime*) dan dapat dilihat pada Gambar 1.



Gambar 1. Statistik Kejahatan *Cyber* dalam Skala Global

Menurut data Direktorat Cyber Crime Polri, kejahatan siber di Indonesia tergolong tinggi. Laporan kasus *cybercrime* menguraikan terdapat sebanyak 4.360 kasus pada tahun 2018, 3,429 kasus pada tahun 2019 dan 2.259 kasus sepanjang Januari hingga September 2020. Laporan kasus paling menonjol pada tahun 2020 adalah penyebaran konten provokatif yaitu sebanyak 1.048 kasus. Salah satu penyebab kasus tersebut yaitu penggunaan media sosial berupa berbagai macam aplikasi sepanjang aplikasi tersebut menyediakan fitur layanan IM untuk mengirim pesan teks, gambar maupun video. Salah satu media sosial yang memiliki fitur tersebut adalah *Signal Messenger*. Tindakan kriminal yang dapat ditemukan dari media sosial dengan layanan IM yaitu ujaran kebencian dan penipuan [3]. Tingginya kasus penipuan di media sosial mendorong dilakukannya investigasi kasus penipuan (*cyber fraud*) melalui analisis forensik menggunakan pendekatan atau metode yang umumnya digunakan yaitu *National Institute of Standarts and Technology* (NIST).

Terdapat cukup banyak penelitian terdahulu dalam analisa forensik yang sudah menggunakan metode NIST. Penelitian Riadi, Umar dan Firdonsyah (2017) pada *Blacberry messenger* diperoleh hasil berupa rekaman percakapan, nama dan PIN pengirim pesan, isi pesan, tipe dan waktu pengiriman pesan sebagai barang bukti yang berhubungan dengan kasus *cybercrime*, namun bukti gambar tidak dapat dimunculkan gambar [4]. Penelitian pada aplikasi Whatsapp diperoleh bukti digital berupa Whatsapp *contact list*, *log* panggilan WA dan pesan teks serta gambar melalui *Whatsapp Key/DB Extractor* [5]. Sementara *Belkasoft Evidence* mendapatkan dokumen gambar dan video, sedangkan *Oxygen Forensic* mampu menghasilkan list contact, pesan teks (pengirim dan penerima pesan, isi pesan dan waktu pengiriman pesan), gambar dan video. Penelitian pada aplikasi Instagram memperoleh bukti digital berupa percakapan (*chat*) dan gambar [6].

Penelitian pada *facebook messenger* (2018) mendapatkan bukti digital berupa teks dan waktu pengiriman percakapan, gambar dan audio [7]. Penelitian metode NIST juga digunakan pada penelitian analisis bukti pada aplikasi WhatsApp *mobile* [8] dan *facebook facebook Lite* [9]. Penelitian lain tentang analisis forensik dengan metode NIST pada aplikasi *WhatsApp* didapakan isi percakapan (*chat*), nomor kontak, waktu percakapan (tanggal, bulan, tahun, jam), serta semua nomor kontak di WA pelaku *cybercrime* [10]. Sementara itu, penelitian lain mengenai analisis forensic pada smartphone dengan menggunakan metode NIST dan *tool MobileEdit forensic Express* memperoleh bukti fisik berupa profil pengguna, kontak, pesan, panggilan, foto dan gambar sebanyak 75% [11].

Penelitian yang dilakukan oleh Riadi, dkk tentang analisis forensik dengan metode NIST pada viber *messenger* android juga memperoleh bukti digital berupa kontak, akun, gambar dan video dengan

persentase 100%. Sedangkan bukti digital *chat* dengan persentase 50%. Hasil tersebut diperoleh dengan menggunakan *tools MOBILedit Forensic* dan *belkasoft* [12]. Penelitian yang dilakukan tentang analisis dukti digital pada telegram messenger menggunakan framework NIST memperoleh bukti berupa percakapan antara pelaku dan korban penipuan [13]. Lebih lanjut, penelitian yang dilakukan oleh Indriyanto, Hariyadi dan Habibi membuktikan hasil analisis forensik percakapan pada grup *instant messenger* dengan metode NIST memperoleh konten negatif sebanyak 96,21% [14].

Ramadhan & Riadi (2019) dalam penelitiannya menunjukkan bahwa analisis forensik pada *WhatsApp* dengan metode NIST menemukan bukti berupa 11 database percakapan enkripsi, 1 database percakapan deskripsi, 152 gambar diterima, 60 gambar terkirim, waktu dan catatan 8 video, 3 folder pesan suara, 1 dokumen terkirim dan 3 dokumen diterima [15]. Riadi, dkk juga membuktikan bahwa analisis forensic dengan metode NIST dengan *tool* Oxygen mampu melakukan *back up* data (ID, arah pesan, pihak yang terlibat, teks dan waktu) dengan index analisis sebesar 61,9%, sedangkan pada *MOBILedit forensic tool* diperoleh bukti dengan indeks analisis sebesar 76,19% [16]. Selain itu, suatu penelitian yang dilakukan oleh Riadi, dkk tentang analisis forensik pada media sosial Linkedln dengan menggunakan metode NIST dan MOBILedit *forensic tool* memperoleh bukti berupa aktivitas *log*, *update status*, 17 *password WiFi*, 117 riwayat *download*, 263 panggilan telepon, 1 *file* yang telah terhapus, 1 *file* tersembunyi, dan 1 *file* dimunculkan [17].

Penelitian yang dilakukan oleh Mahajan, dkk membuktikan hasil analisis fornsik dengan metode NIST pada WhatsApp dan Viber diperoleh bukti berupa riwayat *chat,* pesan, gambar yang terkirim dan diterima, lokasi *file* video di kartu memori, daftar kontak, detail panggilan [18]. Penelitian yang dilakukan oleh Sunardi, dkk menunjukkan bahwa 100% hasil analisis forensik pada aplikasi *WhatsApp* menggunakan *Wondershare Dr. Fone* mampu menemukan data foto, video, kontak, dan dokumen [19]. Penelitian ini memilih aplikasi *Signal Messenger* sebagai objek penelitian. Serangkaian proses forensik menggunakan metode NIST dilakukan untuk mendapatkan barang bukti digital berupa data teks percakapan (chat), gambar, GIF, dokumen berupa PDF, video, *voice call* dan *video call*.

2. Metode Penelitian

2.1. Alat dan *Software* Pendukung Penelitian

Penelitian ini menggunakan alat dan *software* untuk mendukung proses analisis forensik. Alat yang digunakan antara lain *smartphone* Xiaomi Redmi 9T, laptop Lenovo AMDA Ryzen 3, dan USB connector. *Software* pendukung pada penelitian analisis forensik ini yaitu *signal messenger* dan *MOBILedit Forensic Express*. Proses pencarian dan pengambilan barang bukti digital membutuhkan sumber daya yang besar sehingga dibutuhkan perangkat pendukung agar proses tersebut dapat berjalan dengan lancar dan tepat. Pemilihan android *smartphone* disesuaikan dengan kebutuhan penelitian karena memiliki spesifikasi yang memenuhi syarat dari segi sumber daya yang besar. Spesifikasi android Xiaomi Redmi 9T unggul dari segi sumber daya, RAM, CPU *speed* dan memiliki slot memori eksternal jika dibandingkan *device* yang setipe termasuk iPhone. *Smartphone* Xiaomi Redmi 9T juga bersifat *open source* dan menggunakan prosesor snapdragon sehingga lebih memudahkan dalam proses *root*. *Rooting* mempermudah pengangkatan data-data yang ada di dalam perangkat android. Spesifikasi yang memenuhi syarat, proses *root* yang benar dan kemampuan *tool* forensik mempengaruhi hasil dalam pengangkatan bukti digital. Alat dan *software* pendukung yang digunakan dalam penelitian analisis forensik *cyber fraud* pada *Signal Messenger* menggunakan metode NIST dapat dilihat pada Tabel 1.

Tabel 1. Alat dan *Software* Pendukung Penelitian

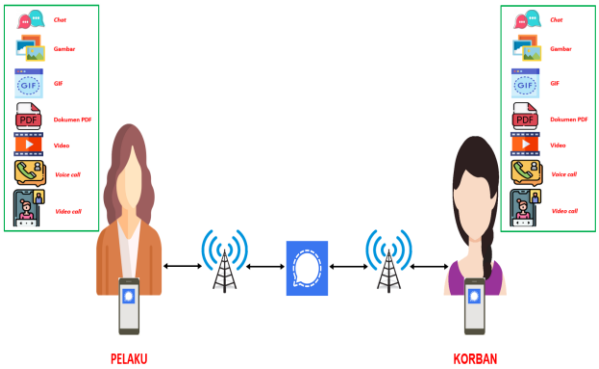
No.	Alat dan *Software*	Deskripsi
1	Xiaomi Redmi 9T	*Rooted*, Objek penelitian
2	Laptop Lenovo AMDA Ryzen 3	Windows 10 64 Bit 8.00 GB RAM, *Workstation* untuk analisis forensik
3	USB *Connector*	Media penghubung *smartphone* dan *workstation*
4	*Signal Messenger*	*Software test*
5	*MOBILedit Forensic Express*	*Tool forensic*

2.2. Perancangan Sistem

Pada penelitian ini, *smartphone* sudah dalam keadaan di *rooted*. Rancangan sistem dimulai dengan membuat sebuah skenario rekayasa yang dijalankan untuk mendapatkan bukti digital. Pada penelitian ini, dibuat skenario lengkap dengan aktivitas yang dilakukan pada aplikasi *Signal Messenger*. Skenario diawali dengan pembahasan jual beli properti berupa rumah kosan. Pelaku dan korban membahas tentang kondisi rumah, sertifikat dan alamat lengkap rumah. Pada akhir percakapan terdapat jeda waktu sekitar 5 jam 38 menit saat korban menanyakan tentang kejelasan rumah tetapi tidak mendapatkan balasan dari pelaku.

Skenario dibuat dengan tujuan untuk mempermudah investigasi kasus penipuan. Skenario tersebut yaitu: pertama, pelaku membuat akun *signal messenger* (akun A) di *smartphone* android. Kedua, pelaku melakukan *chatting* terhadap korban/akun B (kondisi normal). Ketiga, pelaku mengirimkan gambar kepada korban (kondisi normal). Keempat, pelaku mengirimkan *chatting* berisi konten penipuan kepada korban. Kelima, pelaku mengirimkan gambar berisi konten penipuan. Terakhir, pelaku menghapus semua data *chat*, gambar, GIF, Dokumen berupa PDF, video,

audio call maupun *video call* berisi konten penipuan dari perangkat pelaku. Data teks percakapan terhapus dari *signal messenger* akan diungkap dari perangkat *smartphone* si pelaku menggunakan *tools* forensik. Adapun skenario dapat dilihat pada Gambar 2.

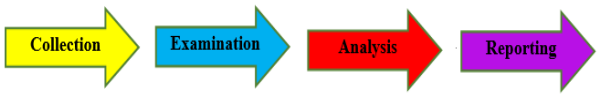


Gambar 2. Skenario Kasus Penipuan

Berdasarkan skenario di atas terlihat ada dua pengguna *smartphone* yang menggunakan aplikasi *signal messenger* untuk berkomunikasi. Akun A sebagai pelaku melakukan tindakan penipuan (*cyber fraud*) terhadap pengguna lainnya yang disebut korban (akun B). Pelaku mengirim pesan kepada korban dan melalui jaringan internet dan akan sampai pada server. *Signal Messenger* kemudian diteruskan ke korban. Dari tindakan penipuan tersebut akan diidentifikasi barang bukti berupa profil pengguna akun pelaku dan hasil percakapan baik berupa pesan teks, gambar, GIF, dokumen berupa PDF, video, *voice call* ataupun *video call* antara korban dan pelaku oleh investigator.

2.3. Pengujian Sistem

Skenario yang dirancang dilanjutkan ke tahap uji coba atau simulasi. Hasil simulasi kemudian dianalisis menggunakan metode *National Institute of Standart and Technology* (NIST). Metode NIST memiliki beberapa tahap seperti terlihat pada Gambar 3.



Gambar 3. Tahapan Metode NIST

Metode NIST terdiri dari 4 tahap yaitu *collection*, e*xamination*, *analysis*, dan *reporting* [20]. *Collection* merupakan tahapan dilakukannya proses identifikasi, pelabelan, perekaman dan pengambilan data dari sumber data yang relevan berdasarkan prosedur yang tepat sehingga dapat mempertahankan keaslian data dan menjaga integritas data. *Examination* merupakan tahapan dilakukannya pengolahan atau pemrosesan data yang dikumpulkan secara forensik menggunakan kombinasi beberapa skenario baik manual ataupun otomatis, kemudian menilai dan mengeluarkan data sesuai kebutuhan penelitian. Proses pemeriksaan terhadap data barang bukti menggunakan *tools* forensik untuk menjaga integritas data.

Analysis merupakan tahapan dilakukannya pemeriksaan hasil dari proses *examination* sesuai prosedur hukum dengan tujuan untuk mendapatkan informasi yang dapat digunakan. Data bukti digital yang diperoleh di tahap *examination* dianalisis guna membuat kesimpulan dari bukti digital. File hasil yang relevan akan dibuka dan dianalisis menggunakan *tools* forensik. *Reporting* merupakan tahapan pelaporan hasil analisis yang mencakup prosedur tindakan yang diambil, penjelasan alat dan prosedur yang dipilih, penentuan tindakan lain yang diperlukan seperti pemeriksaan forensik dari sumber data tambahan atau peningkatan kontrol keamanan, serta hasil yang diperoleh dari penelitian. Pihak investigator melaporkan hasil investigasi atau penyelidikan beserta bukti digital yang ditemukan. Laporan bukti digital yang berhasil disusun sesuai skenario yang dirancang.

3. Hasil dan Pembahasan

Penelitian ini merupakan hasil simulasi kasus berdasarkan skenario yang telah dirancang sebelumnya. Penelitian analisis forensik pada aplikasi *signal messenger* mengangkat kasus *cyber fraud* yang dilakukan salah seorang makelar jual beli properti. Metode yang digunakan dalam penelitian ini yaitu metode NIST dengan tahap *collection*, *examination*, *analysis,* dan *reporting*.

3.1. *Collection*

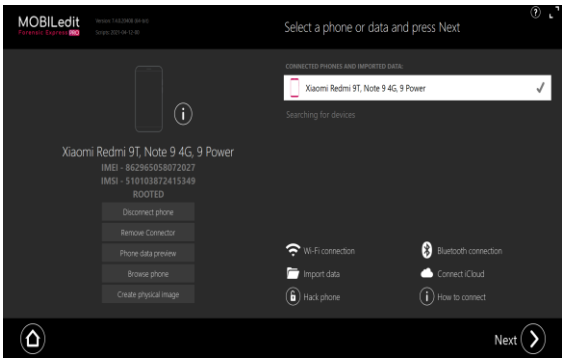
Pada tahap ini dilakukan akuisisi atau pengambilan barang bukti. Barang bukti berupa *smartphone* android yang akan dianalisis yaitu sebuah *smartphone* Xiaomi Redmi 9T. *Smartphone* android dalam kondisi sudah di *rooted* dan sudah di *custom* ROM. Barang bukti *smartphone* android ditunjukkan oleh Gambar 4. Selanjutnya dilakukan pengajuan solusi untuk mengembalikan data yang telah dihapus berupa 9 *chats*, 2 gambar, 1 GIF, 1 video, 1 dokumen Pdf, 1 *voice call* dan 1 *video call* menggunakan *tool MOBILedit Forensic Express.*

Gambar 4. *Smartphone* yang Digunakan

3.2. *Examination*

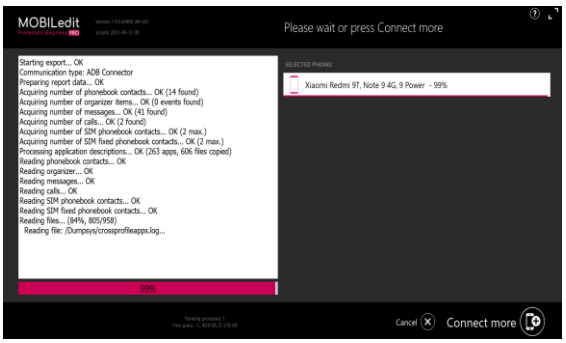
Pada tahap ini dilakukan proses pemeriksaan terhadap data barang bukti. Pemeriksaan dilakukan dengan menggunakan *tool MOBILedit Forensic Express*.

Langkah awal pada tahap *examination* yaitu menonaktifkan saluran data *smartphone* (*airplane mode on*), selanjutnya menghubungkan kabel data dari *smartphone* ke laptop.



Gambar 5. Proses *Examination*

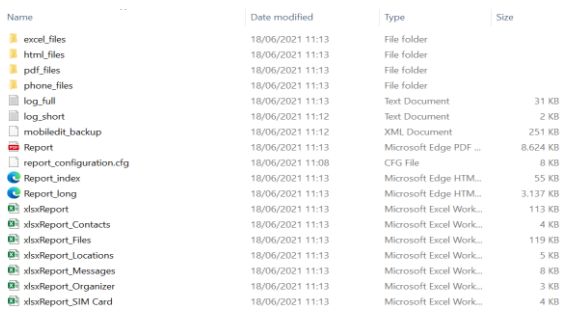
MOBILedit Forensic Express merupakan *software* yang digunakan untuk mengangkat bukti digital. *Tool* forensik ini dapat mengangkat bukti digital pada *smartphone* android dengan cepat dan mudah. Setelah proses awal *examination* seperti terlihat pada Gambar 5, dilakukan pengamanan data dengan cara melakukan *backup* data. Proses *backup* dapat dilihat pada Gambar 6.



Gambar 6. Proses *Backup*

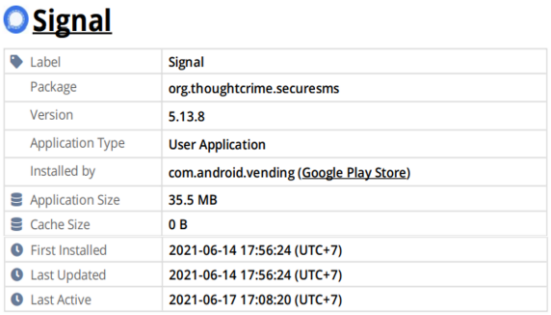
3.3. *Analysis*

Tahap *analysis* merupakan tahapan yang dilakukan untuk melihat hasil dari pemeriksaan atau *examination* secara detail. Pada tahap ini dilakukan pemeriksaan hasil dari proses *examination* sebelumnya untuk mendapatkan bukti digital. Hasil *examination* *MOBILedit Forensic Express* ditunjukkan oleh Gambar 7.



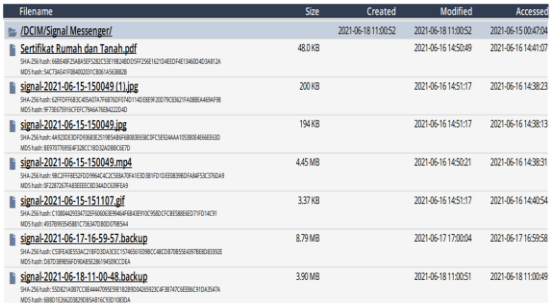
Gambar 7. Hasil *Examination*

MOBILedit Forensic tidak dapat mendekripsi *file* pada aplikasi *Signal Messenger* sehingga tidak diperoleh hasil yang maksimal saat dilakukan *examination*. Aplikasi *signal messenger* harus membuat folder cadangan lokal sendiri, tidak seperti WA dan aplikasi lainnya yang secara otomatis memiliki folder penyimpanan di *internal storage*. Hasil yang didapatkan dari aplikasi *Signal Messenger* ditunjukkan Gambar 8.



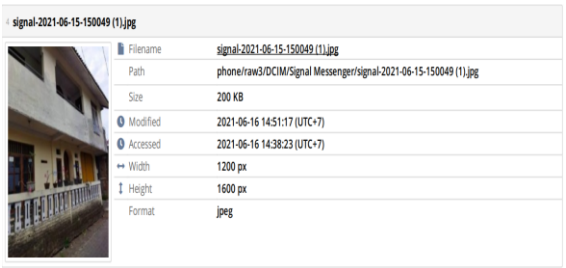
Gambar 8. Barang Bukti Informasi Aplikasi *Signal Messenger*

Hasil dari aplikasi *signal messenger* hanya berupa versi aplikasi, ukuran aplikasi, waktu instalasi, waktu terakhir *update* dan waktu terakhir aktif. Hasil ekstraksi menggunakan *tool* ini juga dapat menampilkan cadangan lokal *signal messenger*. Gambar 9 merupakan tampilan cadangan lokal *signal messenger*.



Gambar 9. Barang Bukti Cadangan Lokal *Signal Messenger*

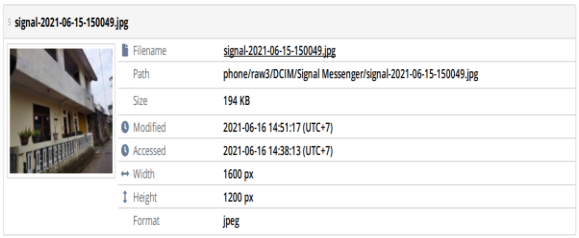
Langkah selanjutnya yaitu mencari barang bukti gambar, GIF, video dan barang bukti lainnya. Berdasarkan hasil ekstraksi diperoleh barang bukti berupa gambar. Terdapat 2 file gambar hasil *reporting* *MOBILedit Forensic Express*.



Gambar 10. Barang Bukti Gambar Pertama

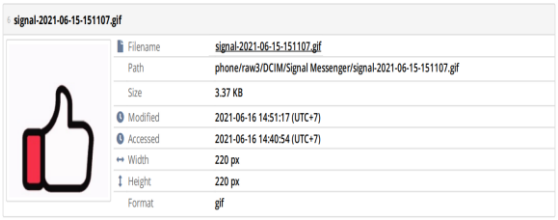
File gambar menunjukkan tampilan luar rumah dari simulasi kasus *cyber fraud.* File gambar pertama hasil

reporting ditunjukkan oleh Gambar 10. Gambar kedua hasil *reporting* dapat dilihat pada Gambar 11.



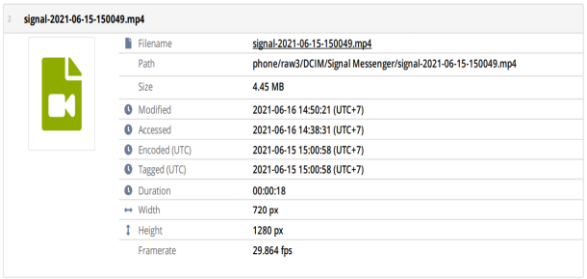
Gambar 11. Barang Bukti Gambar Kedua

Berdasarkan hasil *examination* ditemukan barang bukti berupa *Graphics Interchange Format* (GIF). Terdapat 1 GIF dari hasil *reporting MOBILedit Forensic Express.* Barang bukti GIF ditunjukkan Gambar 12.



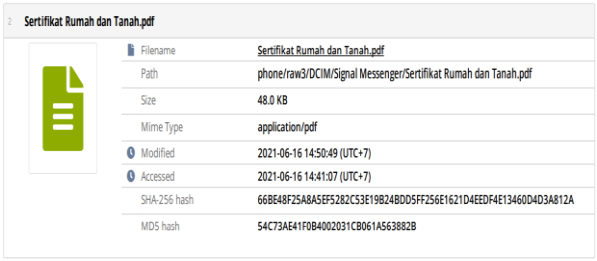
Gambar 12. Barang Bukti GIF

Barang bukti berupa video juga dapat ditemukan melalui simulasi pengangkatan barang bukti pada *smartphone* android. Pengangkatan barang bukti menghasilkan satu video. Gambar 13 menampilkan video hasil *reporting MOBILedit Forensic Express*.



Gambar 13. Barang Bukti Video

Berdasarkan hasil *examination* ditemukan satu dokumen dalam format pdf. Format dokumen seperti pdf, doc, dan zip dapat dibaca oleh *tool MOBILedit Forensic Express*. Barang bukti dokumen pdf hasil *reporting* dapat dilihat pada Gambar 14. Salah satu kekurangan *tool* ini yaitu tidak dapat membaca teks percakapan (chat), *voice call* dan *video call history*.



Gambar 14. Barang Bukti Dokumen PDF

3.4. *Reporting*

Setelah dilakukan simulasi berdasarkan skenario dan dilakukan analisis sesuai tahapan forensik NIST terhadap aplikasi *signal messenger* maka dapat disimpulkan proses investigasi berlangsung dengan cukup baik sehingga mampu mengangkat beberapa barang bukti digital pada aplikasi *Signal Messenger*. Berdasarkan hasil forensik, dari 2 data asli gambar diperoleh 2 bukti digital gambar. Data asli GIF pada android sebanyak 1 dan diperoleh 1 bukti digital GIF. Data asli dokumen pdf pada android sebanyak 1 dan diperoleh 1 bukti digital dokumen pdf. Data asli video pada android sebanyak 1 dan diperoleh 1 bukti digital video. Masing-masing persentase keberhasilan untuk gambar, GIF, dokumen pdf dan video sebesar 100%. Sedangkan untuk data chat, *voice call* dan *video call history* tidak dapat dibaca atau tidak dapat ditemukan. Bukti digital secara rinci dapat dilihat pada Tabel 2.

Tabel 2. *Reporting* Bukti Digital

Bukti Digital	Jumlah	Persentase
Chat	9	0%
Gambar	2	100%
GIF	1	100%
Dokumen Pdf	1	100%
Video	1	100%
Voice call	1	0%
Video call	1	0%

Persentase untuk bukti digital chat, *voice call* dan *video call history* sebesar 0%. Kurangnya kemampuan *tool* forensik *MOBILedit* serta ketidakmampuan dalam mengembalikan data yang hilang menjadi alasan dan kekurangan *tool* forensik sehingga tidak dapat membaca data *chat*, *voice call* dan *video call history*. Perbandingan antara bukti digital yang diperoleh dengan keseluruhan bukti digital yang dicari memperoleh hasil yaitu sebesar 57,14%. *Tool MOBILedit Forensic Express* memiliki tingkat keberhasilan secara keseluruhan sebesar 57,14% karena hanya mampu menemukan 4 dari 7 parameter bukti digital yang dicari. Perolehan tingkat keberhasilan di atas 90% tergantung pemilihan *tool* forensik yang akan digunakan dan kemampuan *tool* forensik tersebut.

4. Kesimpulan

Berdasarkan hasil yang didapatkan dari proses penelitian pada kasus *cyber fraud Signal Messenger* menggunakan metode NIST maka diperoleh barang bukti sebagai pendukung penyelidikan tindak kejahatan di pengadilan. *MOBILedit Forensic Express* mendapatkan bukti digital berupa 2 gambar, 1 GIF, 1 dokumen pdf, dan 1 video. Secara keseluruhan, barang bukti yang dapat diangkat menggunakan *tools* ini memiliki tingkat keberhasilan sebesar 57,14%. Hasil penelitian yang diperoleh sesuai dengan tujuan penelitian yang diharapkan. Dari hasil analisis forensik juga ditemukan kekurangan dari *tool MOBILedit*

Forensic. *Tool* forensik tidak mampu membaca *chats*, *voice call and video call history* serta tidak bisa mengembalikan data yang telah hilang. Selanjutnya akan dilakukan penelitian menggunakan *tool* forensik lainnya untuk memperoleh hasil bukti digital yang lebih maksimal guna kepentingan penyelidikan kasus tindak kejahatan digital.

Daftar Pustaka

[1] M. A. Harahap and S. Adeni, "Tren Penggunaan Media Sosial Selama Pandemi di Indonesia," *J. Prof. FIS UNIVED*, vol. 7, no. 2, 2020.

[2] A. P. U. Siahaan, "Pelanggaran Cybercrime dan Kekuatan Yurisdiksi di Indonesia," *J. Tek. dan Inform.*, vol. 5, no. 1, 2018.

[3] M. S. Asyaky, N. Widiyasono, and R. Gunawan, "Analisis dan Perbandingan Bukti Digitak Aplikasi Instant Messenger pada Android," *J. Penelit. Tek. Inform.*, vol. 3, no. 1, 2018.

[4] I. Riadi, R. Umar, and Firdonsyah, "Identification of Digital on Android's Blackberry Messanger Using NIST Mobile Forensic Method," *Int. J. Comput. Sci. Inf. Secur.*, vol. 15, no. 5, pp. 155 – 160, 2017.

[5] R. Umar, I. Riadi, and G. M. Zamroni, "A Comparative Study of Forensic Tools for WhatsApp Analysis using NIST Measurements," *Int. J. Adv. Comput. Sci. Appl.*, vol. 8, no. 17, pp. 69 – 75, 2017.

[6] I. Riadi, A. Yudhana, and M. C. F. Putra, "Forensic Tool Comparison on Instagram Digital Evidence Based on Android with The NIST Method," *Sci. J. Informatics*, vol. 5, no. 2, pp. 235–247, 2018.

[7] A. Yudhana, I. Riadi, and I. Anshori, "Analisis Bukti Digital Facebook Messenger Menggunakan Metode NIST," *IT J. Res. Dev.*, vol. 3, no. 1, pp. 13–21, 2018.

[8] Yuliani and I. Riadi, "Forensic Analysis WhatsApp Mobile Application on Android-Based Smarthphones using National Institute of Standard and Technology (NIST) Framework," *Int. J. Cyber-Security Digit. Forensics*, vol. 8, no. 3, pp. 223–231, 2019.

[9] R. A. K. N. Bintang, R. Umar, and A. Yudhana, "Analisis Media Sosial Facebook Lite dengan Tools Forensik Menggunakan Metode NIST," *Techno*, vol. 21, no. 2, pp. 125–130, 2020.

[10] M. Fitriana, Khairan, and J. M. Marsya, "Penerapan Metode National Institute of Standards and Technology (NIST) dalam Analisis Forensik Digital Untuk Penanganan Cyber Crime," *Cybersp. J. Pendidik. Teknol. Inf.*, vol. 4, no. 1, 2020.

[11] Nasirudin, Sunardi, and I. Riadi, "Analisis Forensik Smartphone Android Menggunakan Metode NIST dan Tool MOBILedit Forensic Express," *J. Inform. Univ. Pamulang*, vol. 5, no. 1, pp. 89–94, 2020.

[12] I. Riadi, R. Umar, and M. I. Syahib, "Akuisisi Bukti Digital Viber Messenger Android Menggunakan Metode National Institute of Standards and Technology (NIST)," *J. Resti (Rekayasa dan Teknol. Informasi)*, vol. 5, no. 1, pp. 45–54, 2021.

[13] S. Azizah, S. A. Ramadhona, and K. W. Gustitio, "Analisis Bukti Digital pada Telegram Messenger Menggunakan Framework NIST," *Repositor*, vol. 2, no. 10, 2020.

[14] M. W. Indriyanto, D. Hariyadi, and M. Habibi, "Investigasi dan Analisis Forensik Digital pada Percakapan Grup WhatsApp Menggunakan NIST SP 800-86 dan Support Vector Machine," *CyberSecurity dan Forensik Digit.*, vol. 3, no. 2, pp. 34–38, 2020.

[15] M. I. Ramadhan and I. Riadi, "Forensic WhatsApp Based Android Using National Institute of Standard Technologi (NIST) Method," *Int. J. Comput. Appl.*, vol. 177, no. 8, 2019.

[16] I. Riadi, A. Fadlil, and A. Fauzan, "A Study of Mobile Forensic Tools Evaluation on Android-Based LINE Messenger," *Int. J. Adv. Comput. Sci. Appl.*, vol. 9, no. 10, pp. 201–206, 2018.

[17] I. Riadi, A. Yudhana, and M. Al Barra, "Forensik Mobile pada Layanan Media Sosial LinkedIn," *JISKa*, vol. 6, no. 1, pp. 9–20, 2021.

[18] A. Mahajan, M. S. Dahiya, and H. P. Sanghvi, "Forensic Analysis of Instant Messenger Applications on Android Devices," *Int. J. Comput. Appl.*, vol. 68, no. 8, 2013.

[19] Sunardi, I. Riadi, and J. Triyanto, "Forensic Mobile Layanan WhatsApp pada Smartwatch Menggunakan Metode National Institute of Justice," *J. Inf. Technol. Comput. Sci.*, vol. 6, no. 2, 2021.

[20] A. Yudhana, I. Riadi, and I. Anshori, "Analisis Forensik Aplikasi Instant Messenger pada Smartphone Berbasis Android," *J. Insa. Comtech*, vol. 2, no. 2, 2017.

Halaman ini sengaja dikosongkan